Claims

[c1] 1. In a system for performing an action, in response to an electronic communication regarding an account, which electronic communication is received from a sender by a receiver, a method comprising the steps of:

(a)initially, associating by the receiver, sender identity information and a public key of a public-private key pair with the account such that the public key is retrievable based on the sender identity information, and wherein the public key is associated with the account in a computer database; and thereafter

(b)receiving the electronic communication from the sender,

(i)wherein the electronic communication was created after the association of the sender identity information and the public key with the account in step (a),

(ii)wherein the electronic communication comprises,

(A)the sender identity information, and

(B)predetermined encoded information obtained by using the private key of the pair, and (iii)wherein the electronic communication is communicated electronically from the sender; and

(c)validating the identity of the sender for the electronic communication by only performing the steps of,

(i)utilizing the sender identity information received in the electronic communication to retrieve the public key based on the association of the sender identity information and the public key with the account performed in step (a), and

(ii)comparing a function of the public key and the predetermined encoded information with a function of the electronic message, wherein the function comprises decrypting the predetermined encoded information using the public key,

whereby a comparison resulting in a match validates the identity of the sender.

[c2] 2. In a system for performing an action, in response to an electronic communication regarding an account, which electronic communication is received from a sender by a receiver, a method comprising the steps of:

(a)initially, associating by the receiver, sender identity information and a public key of a public-private key pair with the account such that the public key is retrievable based on the sender identity information, and wherein the public key is associated with the account in a computer database; and thereafter

(b)receiving the electronic communication from the sender,

(i)wherein the electronic communication was created after the association of the sender identity information and the public key with the account in step (a),

(ii)wherein the electronic communication comprises,

(A)the sender identity information, and

(B)predetermined encoded information derived using the private key of the pair, and

(iii)wherein the electronic communication is communicated electronically from the sender; and

(c)validating the identity of the sender for the electronic communication by,

(i)utilizing the sender identity information received in the electronic communication to retrieve the public key based on the association of the sender identity information and the public key with the account performed in step (a), and

(ii)comparing a function of the public key and the predetermined encoded information with a function of the electronic message, wherein the function comprises decrypting the predetermined encoded information using the public key,

whereby a comparison resulting in a match validates the identity of the sender, and wherein neither a PIN nor a password is required to be transmitted to the receiver for validating the identity of the sender.

[c3] 3. In a system for performing an action, in response to an electronic communication regarding an account, which electronic communication is received from a sender by a receiver, a method comprising the steps of:

(a) initially, associating by the receiver, sender identity information and a public key of a public-private key pair with the account such that the public key is retrievable based on the sender identity information, wherein the sender identity information comprises other than an account number, and wherein the public key is associated with the account in a computer database; and thereafter

(b) receiving the electronic communication from the sender,

(i)wherein the electronic communication was created after the association of the sender identity information and the public key with the account in step (a),

(ii)wherein the electronic communication comprises,

(A)the sender identity information, and

(B)predetermined encoded information derived using the private key of the pair, and

(iii)wherein the electronic communication is communicated electronically from the sender; and

(c)validating the identity of the sender for the electronic communication by,

(i)utilizing the sender identity information received in the electronic communication to retrieve the public key based on the association of the sender identity information and the public key with the account performed in step (a), and

(ii)comparing a function of the public key and the predetermined encoded information with a function of the electronic message, wherein the function comprises decrypting the predetermined encoded information using the public key,

whereby a comparison resulting in a match validates the identity of the sender.

[c4] 4. In a system for performing an action, in response to an electronic communication regarding an account, which electronic communication is received from a sender by a receiver, a method comprising the steps of:

(a)initially, associating by the receiver, sender identity information and a public key of a public-private key pair with the account such that the public key is retrievable based on the sender identity information, and wherein the public key is associated with the account in a computer database; and thereafter

(b)receiving the electronic communication from the sender,

(i)wherein the electronic communication was created after the association of the sender identity information and the public key with the account in step (a),

(ii)wherein the electronic communication comprises,

(A)the sender identity information, and

(B)predetermined encoded information derived using the private key of the pair,

(iii)wherein the electronic communication is communicated electronically from the sender, and

(iv)wherein the electronic communication is the only electronic communication received from the sender by the receiver relating to the action; and

(c)validating the identity of the sender for the electronic communication by,

(i)utilizing the sender identity information received in the electronic communication to retrieve the public key based on the association of the sender identity information and the public key with the account performed in step (a), and

(ii)comparing a function of the public key and the predetermined encoded information with a function of the electronic message, wherein the function comprises decrypting the predetermined encoded information using the public key,

whereby a comparison resulting in a match validates the identity of the sender.

[c5] 5.The method of claims 1, 2, 3, or 4, wherein the predetermined encoded information comprises transactional account information.

[c6] 6.The method of claims 1, 2, 3, or 4, wherein the predetermined encoded information comprises entity information.

[c7] 7.The method of claims 1, 2, 3, or 4, wherein the ac-

count information comprises transactional account information.

[c8] 8.The method of claims 1, 2, 3, or 4, wherein the account information comprises entity information.

[c9] 9.The method of claims 1, 2, 3, 4, 5, 6, 7, or 8, wherein the electronic communication includes the electronic message.

[c10] 10.The method of claims 1, 2, 3, 4, 5, 6, 7, or 8, wherein the electronic message is implied from the receipt of the electronic communication.

[c11] 11.The method of claims 1, 2, 3, 4, 5, 6, 7, or 8, wherein the digital signature is derived within a smart card of the sender.

[c12] 12.The method of claims 1, 2, 3, 4, 5, 6, 7, or 8, wherein the predetermined encoded information is received from the sender within a terminal of a third-party and then forwarded to the receiver.

[c13] 13.The method of claims 1, 2, 3, 4, 5, 6, 7, or 8, wherein the electronic communication is received over a secure network.

[c14] 14.The method of claims 1, 2, 3, 4, 5, 6, 7, or 8, wherein the electronic communication is received over an inse-

cure network.

[c15] 15.The method of claim 14, wherein the network comprises the Internet.

[c16] 16.The method of claims 1, 2, 3, 4, 5, 6, 7, or 8,wherein the electronic communication is received encrypted.

[c17] 17.The method of claims 1, 2, 3, 4, 5, 6, 7, or 8, wherein the electronic communication is received unencrypted.

[c18] 18.The method of claims 1, 2, 3, 4, 5, 6, 7, or 8, wherein the receiver is a financial institution and the action on the account comprises a financial transaction.

[c19] 19.The method of claims 1, 2, 3, 4, 5, 6, 7, or 8, wherein the electronic communication includes the public key.

[c20] 20.The method of claims 1, 2, 4, 5, 6, 7, or 8, wherein the sender identity information comprises the account number.

[c21] 21.The method of claims 1, 2, 4, 5, 6, 7, or 8, wherein the sender identity information comprises other than the account number.

[c22] 22.The method of claims 1, 2, 3, 4, 5, 6, 7, or 8, wherein the public key was associated with the account when the account was first established.

[c23] 23.The method of claim 22, wherein the public key was provided by the sender to the receiver.

[c24] 24.The method of claim 22, wherein the public key was provided to the sender by the receiver.

[c25] 25.The method of claims 1, 2, 3, 4, 5, 6, 7, or 8, wherein the predetermined encoded information includes information required to process the action.

[c26] 26.The method of claims 5 or 7, wherein the transactional account information includes a personal identification number (PIN).

[c27] 27.The method of claims 5 or 7, wherein the transactional account information includes an account balance representing funds in the account.

[c28] 28.The method of claims 5 or 7, wherein the transactional account information includes information validated when the account was established.

[c29] 29.The method of claims 5 or 7, wherein the transactional account information includes information that was validated in a face-to-face acknowledgement between the sender and the receiver.

[c30] 30.The method of claims 1, 2, 3, 4, 5, 6, 7, or 8, wherein

the account comprises a checking account.

[c31] 31.The method of claims 5 or 7, wherein the transactional account information includes a history of ledger transactions in the account.

[c32] 32.The method of claims 6 or 8, wherein the entity information includes the social security number of the sender.

[c33] 33.The method of claims 6 or 8, wherein the entity information includes the address of the sender.

[c34] 34.The method of claims 6 or 8, wherein the entity information includes the mother"s maiden name of the sender.

[c35] 35. The method of claims 6, wherein the predetermined encoded information only includes entity information of the sender.

[c36] 36.The method of claims 8, wherein the account information only includes entity information of the sender.

[c37] 37.The method of claims 5 or 7, wherein the transactional account information includes business process information.

[c38] 38.The method of claims 5 or 7, wherein the transac-

tional account information is stored in fields in records in a computer database.

[c39] 39.The method of claim 38, wherein the records comprise an account file.

[c40] 40.The method of claim 39, wherein the records further comprise a transactions file.

[c41] 41.The method of claims 1, 2, 3, or 4, wherein the predetermined encoded information is derived within a hand-held device of the sender.

[c42] 42.The method of claims 6 or 8, wherein the entity information comprises personal information of the sender.

[c43] 43.The method of claims 1, 2, 3, or 4, wherein the function of the electronic message comprises applying a hashing algorithm to the electronic message.

[c44] 44.The method of claims 1, 2, 3, or 4, wherein the function of the public key and the predetermined encoded information is a digital signature.